Last Updated: September 11, 2009

Generally Accepted Privacy Principles

By
James M. Dzierzanowski, Ph.D.

Privacy Introduction

Every organization that handles personal information – whether for consumers, customers, employees or business partners – faces a number of obligations related to privacy and the protection of that information. The current economic environment has added a particularly complex challenge to the ability of companies to manage privacy and protect personal information.

Not too many years ago, privacy was considered more of a telemarketing issue about unwanted phone calls and email messages. In more recent years, privacy has been associated with the potential for abuse – inappropriate access to or exposure of information resulting in identity theft and fraud[1].

A Global Privacy Framework: Generally Accepted Privacy Principles (GAPP)[2]

Many nations, have developed policies akin to the Privacy Act of 1974 within the United States, the 1995 European Data Protection Directive, and the 1997 European Union Telecommunications Privacy Directive, to provide guidance on privacy oversight and address other issues such as trans-border data flow/havens (Safe Harbor). Based on this body of work, the US American Institute of Certified Public Accountants and its Canadian counterpart formed a workgroup to develop common privacy principles, with the end product being GAPP, a series of *10 principles for businesses and individuals* to follow, and they are listed below:

1. Management. The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.

[1] Source: www.ey.com
[2] Source: American Institute of Certified Public Accounts, www.aicpa.org

2. Notice. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

3. Choice and Consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4. Collection. The entity collects personal information only for the purposes identified in the notice.

5. Use and Retention. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.

6. Access. The entity provides individuals with access to their personal information for review and update.

7. Disclosure to Third Parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. Security for Privacy. The entity protects personal information against unauthorized access (both physical and logical).

9. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

10. Monitoring and Enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

The *Generally Accepted Privacy Principles,* en masse, represent the American and Canadian contribution to the effective management of privacy risk. Good privacy is simply a good business practice. We are living in a time when technological, social and political developments threaten, challenge or redefine our privacy "rights" at every turn. In the end, we must know that personal responsibility and foresight are our best tools in combating these concerns.